

AFFIDAVIT OF VA OIG SPECIAL AGENT THOMAS DONNELLY
IN SUPPORT OF SEARCH WARRANT

I, Special Agent Thomas Donnelly, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Veterans Affairs, Office of the Inspector General (VA OIG), where I have been employed since June 2021. Prior to joining VA OIG, I was employed as a Special Agent with the Naval Criminal Investigative Service (NCIS) for approximately six years. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the NCIS Special Agent Basic Training Program. Prior to NCIS, I served as a uniformed police officer for the Department of Defense and the Department of Veterans Affairs.
2. I am currently assigned to the Manchester, NH Resident Agency of the VA OIG. My duties include conducting investigations related to fraud and violations of the Stolen Valor Act as well as related to numerous other violations of Title 18 of United States Code.
3. During my law enforcement career, I have participated in investigations involving fraud, falsified documents, the analysis of electronic devices, and the analysis of cellular telephone data. I have been the affiant, co-affiant, and/or participated in the execution of multiple federal search and arrest warrants pertaining to violations of the federal law.

4. As described below, there is probable cause to believe that SARAH JANE CAVANAUGH (DOB: xx/xx/1991) (“CAVANAUGH”) committed violations of federal law, specifically 18 USC § 498 (Military or Naval Discharge Certificates), 18 USC § 1343 (Fraud by Wire, Radio, or Television), and 18 USC § 704(b)(d)(1) (collectively Military Medals or Decorations) (the “Target Offenses”), and that evidence, fruits, and instrumentalities of the Target Offenses will be found at her residence, on her person, and in vehicles belonging to her (the “Target Locations”), including on CAVANAUGH’s computer devices and cellular phone or phones that are or were previously assigned call number (401) 864-1535 (“Target Device 1”) (collectively, the “Target Devices”).

- a. Target Device 1 is a Verizon Wireless cellular device that is associated with telephone number (401) 864-1535. The make/model is unknown. The investigation to date indicates that the phone number associated with Target Device 1 has been used by CAVANAUGH since September 2010 and was still being used by CAVANAUGH as of February 2022. As of February 2, 2022, this line was still active.

5. I am aware, based on my training and experience, that Title 18, United States Code Section 498 makes it a federal offense for any person to counterfeit, forge, or alter US military discharge papers. Title 18, United States Code Section 1030 makes it a federal offense for any person to use false pretenses to obtain money or property by means of wire communication. Additionally, I am aware that Title

18, Section 704(b)(d)(1) makes it a federal offense for any person to claim receipt of military medals for the purposes of obtaining a tangible benefit.

6. I submit this affidavit in support of an application for a search warrant for the person of SARAH CAVANAUGH, her residence at 26 Corey Avenue, Warwick, RI 02818, and vehicles parked at the residence that are determined to be owned, leased or operated by her, as further described in Attachment A (the "Target Locations"). Based on my investigation, CAVANAUGH resides at this address and has done so since July 28, 2017. As set forth below, there is probable cause to believe that CAVANAUGH has made false statements regarding her military service in order to obtain both monetary and non-monetary benefits, and there is probable cause to believe that the evidence, fruits, and instrumentalities of her violations of 18 USC § 498, 18 USC § 1343, and 18 USC § 704(b)(d)(1), including one or more of the Target Devices and evidence of the Target Offenses contained therein, as more fully described in Attachment B, will be found in her residence, on her person, or in her vehicle(s).
7. Information obtained from a database commonly used by law enforcement shows that CAVANAUGH and Nicole BREGLER – a co-inhabitant with her at 26 Corey Avenue - do have an active lien on a 2019 Volvo S60, color black, Rhode Island registration "202." The lien is associated with both BREGLER and CAVANAUGH, and the address is 26 Corey Ave. RI Department of Motor Vehicle records indicate that BREGLER does not have a RI driver's license, while CAVANAUGH does.

8. The statements contained in this affidavit are based on my participation in this investigation. This affidavit is submitted for the limited purpose of establishing probable cause to believe that the Target Devices and Target Locations contain evidence of the Target Offenses. It therefore does not set forth all the information that I and other law enforcement personnel have obtained during the course of the investigation.

**PROBABLE CAUSE THAT CAVANAUGH COMMITTED
THE TARGET OFFENSES**

9. On January 27, 2022, Wesley Archambault-Beach, the Associate Chief of Patient Services at the Providence, RI Veterans Affairs Medical Center (VAMC), received an inquiry from Chelsey Simoni. Simoni represents the non-profit organization "HunterSeven." This organization conducts research on military-veteran-specific issues. This organization also provides monetary aid to veterans in need of assistance. Simoni stated her organization received a request for help with paying medical bills from CAVANAUGH. Simoni sought assistance in determining if CAVANAUGH was a veteran of the United States Marine Corps (USMC). Archambault-Beach conducted inquiries of various VA databases and found no evidence CAVANAUGH ever served in the USMC. Archambault-Beach advised Simoni of this fact and relayed this information to Veterans Affairs Police Service.
10. Simoni provided copies of medical bills, a medical diagnosis for cancer, and a military discharge certificate (DD-214) in CAVANAUGH's name. The medical

bills showed CAVANAUGH was undergoing cancer treatments at the Dana Farber Institute in Boston, MA. CAVANAUGH alleged she had lung cancer from exposure to burn pits in Iraq/Afghanistan as well as inhaling particulate matter in the aftermath of an Improvised Explosive Device (IED) attack. The DD-214 indicated CAVANAUGH served in the USMC from 2009 to 2016 and achieved the rank of Corporal. Further review of the DD-214 provided by CAVANAUGH identified inconsistencies. CAVANAUGH's alleged discharge date was circa December 2016. However, the DD-214 was signed by a personnel officer in November of 2015. Based on your affiant's experience, DD-214s are signed contemporaneously with the date of discharge. The DD-214 submitted by CAVANAUGH reflects a signing date nearly a year in advance of her alleged discharge date. Additionally, the DD-214 indicated CAVANAUGH served as a Marine Security Guard (MSG). These Marines serve at all US Embassies overseas. Under the block for military education, no mention of MSG training was entered. This DD-214 credited CAVANAUGH with earning a Purple Heart and a Bronze Star with "V" device. The Purple Heart is given to military members who suffer wounds from enemy action. The Bronze Star with "V" device is awarded for heroic actions.

11. Your affiant conducted independent queries of the Defense Personnel Records Information Retrieval System (DPRIS) for CAVANAUGH. As background, DPRIS generally contains digital military service records for members of all branches of the military, excepting the US Coast Guard. Military servicemembers

who were discharged or retired after 1999 are generally contained in this system. Searches are conducted by last name and Social Security Number. No records were found for CAVANAUGH in this system. The DD-214 CAVANAUGH used to attempt to get monetary donations from Simoni and the HunterSeven non-profit was therefore not an authentic document.

12. In a telephone conversation on February 1, 2022, Simoni told your affiant that HunterSeven rescinded the funds they issued to CAVANAUGH based on the information they received from Archambault-Beach and their own suspicions regarding the authenticity of CAVANAUGH's DD-214. Simoni stated she also doubted the authenticity of the Dana Farber cancer treatment bills because when Simoni contacted the institute to attempt to inquire about the balance of the CAVANAUGH's supposed account, Dana Farber Institute stated the patient number was not valid. The bills submitted by CAVANAUGH to HunterSeven were therefore not authentic documents.

13. Simoni believed CAVANAUGH utilized her fictitious military service to obtain cash donations from a variety of individuals not associated with HunterSeven. Simoni identified an active-duty USMC Major who directly donated money to CAVANAUGH, as well as offered her employment. Simoni also stated CAVANAUGH attended classes for free with an organization in Providence, RI called the "Clemente Institute." Open-source research on the Clemente Institute webpage identified CAVANAUGH as an alumnus, using the last name BREGLER. CAVANAUGH's picture was included on the biography page. In the

biography, CAVANAUGH referenced being wounded in action following the explosion of an IED and had to learn how to “retie her shoes.” Based on her status as an alleged veteran, CAVANAUGH traveled to New York City with the Clemente Institute to visit museums. Simoni estimated CAVANAUGH has obtained approximately \$100,000 USD by posing as a military veteran and cancer patient.

14. Your affiant queried the Veterans Benefits Management System (VBMS) to determine if CAVANAUGH ever attempted to obtain benefits from the Department of Veterans Affairs. In November 2018, CAVANAUGH submitted a notice of intent to file for veterans’ benefits. VA Benefits personnel queried the aforementioned DPRIS system in response to CAVANAUGH’s intent filing and determined no records existed of valid military service.
15. Further investigation revealed CAVANAUGH is employed as a licensed social worker at the Providence, RI VAMC. CAVANAUGH did not claim veteran status when she applied for the position. As a VA social worker, CAVANAUGH has access into a variety of medical record databases and is familiar with DD-214s. A review was conducted utilizing the aforementioned cancer diagnoses submitted to Simoni by CAVANAUGH. It was determined that the records were authentic and belonged to an actual veteran patient of the Providence, RI VAMC. However, the real veteran’s name appears to have been changed to CAVANAUGH’s name. The diagnoses of the real veteran and the diagnoses

submitted by CAVANAUGH to obtain money from HunterSeven contained the exact same typographical errors.

16. Several media outlets reported on CAVANAUGH and her alleged military service at various events. For example, CAVANAUGH appeared, in a USMC uniform, at an event dedicating the Purple Heart Trailway in Rhode Island in August 2021. CAVANAUGH also was elected to be the commander of the Veterans of Foreign Wars (VFW) Post 152 in North Kingstown, RI. As background, this veteran's organization is only open to former military service personnel who meet certain criteria. Prospective members must produce evidence of their military status to gain admittance to the organization. CAVANAUGH has appeared in numerous social media posts and media reporting wearing a USMC uniform and/or VFW regalia.
17. At least one social media fundraising effort was initiated on CAVANAUGH's behalf by actual USMC veterans. A group of veterans making a documentary about military service called "Meatgrinder" created fundraising efforts on the web-based fundraising page "GoFundMe" in November 2021. It is unclear how much money these efforts raised for CAVANAUGH. The purpose of the fundraiser was to help CAVANAUGH pay for mounting medical bills related to cancer. The fundraiser additionally identified CAVANAUGH as a Purple Heart and Bronze Star recipient. CAVANAUGH alleged the cancer was directly related to the inhalation of particulate matter following an IED explosion.

**PROBABLE CAUSE THAT EVIDENCE, FRUITS, AND INSTRUMENTALITIES
OF THE TARGET OFFENSES WILL BE FOUND AT THE TARGET LOCATION**

18. Throughout the investigation, your affiant has established on several occasions that the telephone number assigned to Target Device 1 is CAVANAUGH's primary telephone number. CAVANAUGH has used this phone number as a contact number for employment with VA, as well as to communicate with Simoni and others from whom she attempted to – or did - collect donations. This information shows that CAVANAUGH used this cellular phone and phone number to further her fraud activities.

19. CAVANAUGH has resided at the Target Location since at least July 28, 2017.

This information was obtained through tax records from the Town of Warwick, RI. Additionally, this address is used by CAVANAUGH as her official home of record within her VA employment file. Additionally, CAVANAUGH's current RI driver's license indicates this address as her residence.

20. Based on your affiant's training, experience, and information provided by other law enforcement officers, I know that many individuals now carry smartphones. Smartphones can function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Based on your affiant's

training an experience and the facts contained in this affidavit, your affiant believes Target Device 1 may contain evidence, in the form of text messages, emails, phone calls, voicemails, pictures or videos, and other files, of CAVANAUGH's attempts at fundraising money based on fictitious military service.

21. Due to the COVID-19, CAVANAUGH has been teleworking from her residence.

The VA has issued her equipment to work from home. A review of user logs for CAVANAUGH indicated she signed into VA systems as of February 1, 2022. In my experience, individuals who own smart phones and computers generally keep the devices in close proximity to their location. Furthermore, based on my experience, individuals typically store documents in their residence.

22. In your affiant's experience, I have found that people frequently store both current and old, deactivated devices in their homes for extended periods of time, even if they are not being utilized. Although sometimes people turn in their deactivated phones in connection with a "trade-in" for an upgraded phone, I have found that individuals are often reluctant to discard old devices quickly as they contain personal and sensitive information. I therefore believe it likely that additional devices are also being stored at the Target Location.

23. Based on your affiant's knowledge of how individuals create false documents, desktop or laptop computers are often used with computer peripherals like scanners and printers and a variety of software programs, such as MS Paint, Adobe Photoshop, Snagit, and others to alter genuine documents or create false

documents purporting to be genuine. CAVANAUGH submitted suspect documents such as a DD-214, medical bills, and a medical diagnosis to establish her bona fides and collect or attempt to collect money from various organizations and individuals. Additionally, CAVANAUGH's familiarity with the USMC may indicate she conducted internet research on a computer device. Your affiant knows that internet searches and webpages visited can be stored in a cache on the device and are recoverable. I therefore believe it likely that Target Devices in the Target Location will contain evidence of CAVANAUGH's creation of false documents and internet activity related thereto.

BIOMETRIC ACCESS TO DEVICES

24. This warrant permits law enforcement to compel CAVANAUGH to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the

Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the Target Devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Target Devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any Target Devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Sara CAVANAUGH to the fingerprint scanner of the Target Devices found at the Target Locations; (2) hold the Target Devices found at the Target Locations in front of the face of Sara CAVANAUGH and activate the facial recognition feature;

and/or (3) hold the Target Devices found at the Target Locations in front of the face of Sara CAVANAUGH and activate the iris recognition feature, for the purpose of attempting to unlock the Target Devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel Sara CAVANAUGH to state or otherwise provide the password or any other means that may be used to unlock or access the Target Devices. Moreover, the proposed warrant does not authorize law enforcement to compel Sara CAVANAUGH to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Target Devices.

24. Based on multiple open-source media articles, CAVANAUGH is likely in possession of a USMC uniform, to include medals like the Purple Heart and Bronze Star. Certain media accounts identify CAVANAUGH as a Marine Corps Staff Sergeant and depict her clad in a U.S. Marine uniform and attribute remarks



Purple Heart recipient Staff Sgt. Sarah Cavanaugh, of the U.S. Marine Corps, listens to a speech during a dedication for the newly-named "Purple Heart Trail" last Saturday afternoon at the Westerly Elks Lodge.

Consequently, I believe it is likely that these uniform items are stored at her residence or in her vehicle. Additionally, based on my experience, I know such uniforms and awards can be purchased from a variety of online stores, as well as at military installations. Such purchases occasionally require proof of identity and generate receipts or other sales documents. I believe such documents may be stored at or in the Target Locations.

25. Based on the copious amounts of documents pertaining to military service and medical treatments that CAVANAUGH provided to various charities, I believe it is likely these documents are at the Target Locations in either physical or electronic form.

¹ See https://www.independentri.com/news/article_01a382f2-faf3-11eb-aa71-bbdb86784c57.html

CONCLUSION

26. Based on these facts, I submit there is probable cause to believe that Sarah CAVANAUGH knowingly created a forged military discharge paper in violation of 18 USC § 498. Further, there is probable cause to believe CAVANAUGH also used computers, cellular phones, and the internet in furtherance of fraud, in violation of 18 USC § 1343. Finally, I submit there is probable cause to believe CAVANAUGH wore military medals to which she was not entitled in furtherance of committing fraud, in violation of 18 USC § 704(b)(d)(1).
27. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes will be found at and in the residence and vehicle Target Locations, described in Attachment A, and on the Target Devices, as described in Attachment B.
28. I am aware that the recovery of data by a computer forensic analyst takes significant time – just as drugs seized in a narcotics investigation must later be forensically evaluated in a lab, seized digital evidence must also undergo a similar process. For this reason, the “return” inventory will only contain a list of the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

I declare the foregoing is true and correct to the best of my knowledge and belief.



THOMAS DONNELLY
SPECIAL AGENT, VA OIG

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1
by:

(specify reliable electronic means)

Date

Judge's signature

City and State

U.S. Magistrate Judge